INFORMATION SECURITY for the ENTERPRISE

DTS
Enterprise Information Security Office

Security Incident Checklist

Step 1 – Make a Preliminary Assessment of the Incident

- When and where did the security Incident occur?
- What devices or paperwork were lost, stolen or breached?
- If devices were stolen, were they immediately reported to law enforcement?
- If devices or media were stolen or lost, where they encrypted? If so, to what level? (for example: full disk, folder(s), or file(s))
- What potential data might be involved?
  - An individual's name
  - Social Security Number
  - Credit Card Information
  - Financial Data
  - Driver's License Number
  - State Identification Card Number
  - Health Information
  - Any other specific information that might identify an individual
- Can the data be used for fraudulent or other purposes?
- Is there other information at risk?
- How many individuals were affected by the security Incident?

Step 2 – Contact Appropriate People within the State

- IT Director makes the following Security contacts:
  - Chief Information Security Officer, can be reached at (801) 538-3470 or incidents@utah.gov
- CISO makes the following contact:
  - Attorney General's Office
    Note: Richard Hamp is the point of contact for the Attorney General's Office and can be contacted at (801) 281-1222
- IT Director/CISO makes the following contacts:
  - Agency Executive Director/Commissioner
  - Chief Information Officer (CIO), can be reached at (801) 538-3298
- Attorney General's Office makes the following contacts:
  - Agency A.G. representative
  - Department of Public Safety
  - Local/Federal Law Enforcement
- Agency Executive makes the following contacts:
  - Governor's Office
    Note: Tani Downing is the point of contact for the Governor's Office.
  - Governor's Press Officer

Note: If needed, Lisa Roskelley is the is Press Officer for the Governor and can be contacted at (801) 538-1503

Step 3 – Further Evaluate the Scope of the Incident (CISO/A.G. Investigator/CIO)

- Does there appear to be evidence of suspicious behavior or negligence by an employee, contractor or an outside entity?
- Was there criminal intent? If so, does Public Safety need to conduct interviews?
- Does the agency's Human Resource representatives need to be involved?
- Should the agency's employees be briefed on the situation?
- Has a key person within the agency been identified to monitor the progress and communicate actions to the appropriate people identified in Step 2 of this checklist?

Step 4 – Determine Need to Notify Public (Governor's Office/Agency Executive)

- Do state employees need to be informed of the incident?
- Should the public be notified of the incident? If so, consider the following:
  - Develop talking points
    - Key Message
    - Frequently Asked Questions
    - Next steps
  - Press Release
  - Press Conference
  - Contact other states
  - Any National Associations that could assist in communicating the information to the public
- If law enforcement was involved, did the agency consult with them to determine the timing of what and when details of the security Incident could be released to the public?
- Has an individual been designated as the contact person for releasing information?
- Have the communication messages regarding the security Incident been coordinated between the employees, legislators, and the public?
- When does the agency need to notify affected citizens?

Step 5 – Communication to Individuals Potentially Impacted by the Incident (Governor's Office/Agency Executive)

- How are affected individuals going to be notified of the possibility of identity theft?
- Has a notification letter been prepared announcing the incident to the affected individuals? (sample document - Generic Notification Letter)
- Should a fact sheet be provided to the individuals and legislators with the following key elements?
  - Outline the incident
  - Explain the actions currently being taken by the agency
  - Include the contact information (e.g. the toll free number and web site)
  - Any other pertinent information
- Does a toll free number need to be established to address questions from the individuals?
- Does a call center need to be established to handle the calls? (for example: DTS Help Desk)
- Should questions and answers be developed and shared with the individual? (sample document - Generic Questions and Answers)
- Would a web site be beneficial to share information with the individual on the incident and next steps?

- What types of services need to be purchased for affected individuals in order to mitigate the data breach?
- Does a contract need to be setup with one of the credit bureaus (e.g. Equifax, Experian or TransUnion) to provide free credit monitoring for affected individuals?
- How often should the credit bureau track statistics and report any identity thefts to your agency?
- If a contract is established with one of the credit bureaus, how will the information be communicated to the individuals? (sample document - Generic Letter Announcing Credit Report Services)
- Does a reminder letter on the credit services need to be sent to the citizens? (sample document - Generic Reminder Notification)
- When the credit bureau is unable to locate a credit file for an individual, should a notification be sent? (sample document - Individual Info Not Found Credit Report)

Step 6 – Close out the Security Incident (All)

- Was the checklist sufficient for this incident?
- Does the checklist need to be modified?
- Do new sample documents need to developed and added to the checklist?
- Do new security procedures need to be implemented?
- Does access to the affected data need to be restricted?